

**TRANSMITTAL LETTER TO THE UNITED STATES
DESIGNATED/ELECTED OFFICE (DO/EO/US)
CONCERNING A FILING UNDER 35 U.S.C. 371**

JC10 Rec'd PCT/PTO 01 OCT 2001
U.S. APPLICATION NO. (If known, see 37 CFR 1.5)
09/937923

INTERNATIONAL APPLICATION NO
PCT/EP00/02481

INTERNATIONAL FILING DATE
21 March 2000
(21.03.00)

PRIORITY DATE CLAIMED:
30 March 1999
(30.03.99)

TITLE
METHOD FOR GENERATING IDENTIFICATION NUMBERS

APPLICANT(S) FOR DO/EO/US
Joerg SCHWENK; Tobias MARTIN

Applicant(s) herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information

1. ☒ This is a **FIRST** submission of items concerning a filing under 35 U.S.C. 371.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. ☒ This is an express request to begin national examination procedures (35 U.S.C. 371(f)) immediately rather than delay examination until the expiration of the applicable time limit set in 35 U.S.C. 371(b) and PCT Articles 22 and 39(1).
4. ☒ A proper Demand for International Preliminary Examination was made by the 19th month from the earliest claimed priority date.
5. ☒ A copy of the International Application as filed (35 U.S.C. 371(c)(2))
 - a. ☐ is transmitted herewith (required only if not transmitted by the International Bureau).
 - b. ☒ has been transmitted by the International Bureau.
 - c. ☐ is not required, as the application was filed in the United States Receiving Office (RO/US)
6. ☒ A translation of the International Application into English (35 U.S.C. 371(c)(2)).
7. ☒ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371(c)(3))
 - a. ☐ are transmitted herewith (required only if not transmitted by the International Bureau).
 - b. ☐ have been transmitted by the International Bureau.
 - c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
 - d. ☒ have not been made and will not be made.
8. ☐ A translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371(c)(3)).
9. ☒ An oath or declaration of the inventor(s) (35 U.S.C. 371(c)(4)). (UNSIGNED)
10. ☐ A translation of the annexes to the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371(c)(5)).

Items 11. to 16. below concern other document(s) or information included:

11. ☒ An Information Disclosure Statement under 37 CFR 1.97 and 1.98.
12. ☐ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
13. ☒ A **FIRST** preliminary amendment.
☐ A **SECOND** or **SUBSEQUENT** preliminary amendment.
14. ☒ A substitute specification and a marked up version of the substitute specification.
15. ☐ A change of power of attorney and/or address letter.
16. ☒ Other items or information: International Search Report; International Preliminary Examination Report; and Form PCT/RO/101.

Express Mail No.: EL244508211US

U.S. APPLICATION NO. if known, see 37 CFR 1.5

INTERNATIONAL APPLICATION NO
PCT/EP00/02481ATTORNEY'S DOCKET NUMBER
2345/16517. ☒ The following fees are submitted:**Basic National Fee (37 CFR 1.492(a)(1)-(5)):**

Search Report has been prepared by the EPO or JPO \$890.00

International preliminary examination fee paid to USPTO (37 CFR 1.482) \$710.00

No international preliminary examination fee paid to USPTO (37 CFR 1.482) but
international search fee paid to USPTO (37 CFR 1.445(a)(2)) \$740.00Neither international preliminary examination fee (37 CFR 1.482) nor international
search fee (37 CFR 1.445(a)(2)) paid to USPTO \$1,040.00International preliminary examination fee paid to USPTO (37 CFR 1.482) and all
claims satisfied provisions of PCT Article 33(2)-(4) \$100.00

CALCULATIONS | PTO USE ONLY

ENTER APPROPRIATE BASIC FEE AMOUNT = \$ 890Surcharge of \$130.00 for furnishing the oath or declaration later than ☐ 20 ☐ 30 months
from the earliest claimed priority date (37 CFR 1.492(e)). \$

Claims	Number Filed	Number Extra	Rate		
Total Claims	18 - 20 =	0	X \$18.00	\$0	
Independent Claims	1 - 3 =	0	X \$84.00	\$0	
Multiple dependent claim(s) (if applicable)			+ \$280.00	\$	

TOTAL OF ABOVE CALCULATIONS = \$890Reduction by 1/2 for filing by small entity, if applicable. Verified Small Entity statement must
also be filed. (Note 37 CFR 1.9, 1.27, 1.28). \$**SUBTOTAL =** \$890Processing fee of \$130.00 for furnishing the English translation later the ☐ 20 ☐ 30
months from the earliest claimed priority date (37 CFR 1.492(f)). + \$**TOTAL NATIONAL FEE =** \$890Fee for recording the enclosed assignment (37 CFR 1.21(h)). The assignment must be
accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). \$40.00 per property + \$**TOTAL FEES ENCLOSED =** \$890Amount to be
refunded
charged \$

- a. ☐ A check in the amount of \$_____ to cover the above fees is enclosed.
- b. ☒ Please charge my Deposit Account No. 11-0600 in the amount of \$890.00 to cover the above fees. A duplicate copy of this sheet is enclosed.
- c. ☒ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 11-0600. A duplicate copy of this sheet is enclosed.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137(a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:
Kenyon & Kenyon
One Broadway
New York, New York 10004
Telephone No. (212)425-7200
Facsimile No. (212)425-5288

SIGNATURE

Richard L. Mayer, Reg. No. 22,490
NAME

DATE

CUSTOMER NO. 26646

09/937923

JC09 Rec'd PCT/PTO 01 OCT 2001

[2345/165]

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant(s) : Joerg SCHWENK et al.
Serial No. : To Be Assigned
Filed : Herewith
For : METHOD FOR GENERATING IDENTIFICATION
NUMBERS
Art Unit : To Be Assigned
Examiner : To Be Assigned

Assistant Commissioner
for Patents
Washington, D.C. 20231

**PRELIMINARY AMENDMENT AND
37 C.F.R. § 1.125 SUBSTITUTE SPECIFICATION STATEMENT**

SIR:

Please amend without prejudice the above-identified application before
examination, as set forth below.

IN THE TITLE:

Please replace the title with the following:

--METHOD FOR GENERATING IDENTIFICATION NUMBERS--.

IN THE SPECIFICATION AND ABSTRACT:

In accordance with 37 C.F.R. § 1.121(b)(3), a Substitute Specification
(including the Abstract, but without claims) accompanies this response. It is respectfully
requested that the Substitute Specification (including Abstract) be entered to replace the
Specification of record.

Express Mail No. EL244508211US

IN THE CLAIMS:

Without prejudice, please cancel original claims 1 to 17 in the original application, and please add new claims 18 to 35 as follows:

18. (New) A method for generating a personal identification number (PIN) having a number of N decimal digits, to be used for money cards and other security-requiring devices, comprising:

generating the personal identification number from a binary number having L digits so that the personal identification number is randomly distributed over an available number domain.

19. (New) The method of claim 18, further comprising:

converting a first predefinable natural number n_1 of digits of the binary number into a decimal number d_1 ;

wherein:

the first predefinable natural number n_1 of digits is selected so as to yield a natural number z_1 such that a quotient $2^{n_1}/(z_1 * 9)$ is close to 1;

a first decimal digit of the personal identification number receives a value d_1 modulo 9; and

N-1 further groups of a predefinable number n_2 of digits of the binary number are converted each time into N-1 decimal numbers d_2 through d_N , the predefinable number n_2 being selected so as to yield a natural number z_2 such that a quotient $2^{n_2}/(z_2 * 10)$ is close to 1, to satisfy a condition of $0 \leq 2^{n_2} \text{ modulo } 10 < 3$, and decimal digits 2 through N of the personal identification number receive values d_i modulo 10, $i=2$ through N.

20. (New) The method of claim 18, wherein n_1 and $n_2 \leq 16$ are predefined.

21. (New) The method of claim 18, wherein $N=4$ is selected.

22. (New) The method of claim 18, wherein the binary number has a length of $L=16$, and $N=4$ and $n_1=n_2=4$ are predefined.

23. (New) The method of claim 18, wherein the binary number has a length $L=3*n_3$, n_3 groups of three digits of the binary number are converted into n_3 decimal digits to generate n_3 digits of the personal identification number, and n_3 is a natural number.

24. (New) The method of claim 18, wherein the binary number is fully converted into a decimal number to generate the personal identification number, and if necessary, a correction value is added to a resultant decimal number so that a first digit of the decimal number becomes unequal to zero, digits of the resultant decimal number forming the decimal digits of the personal identification number.

25. (New) The method of claim 24, wherein the binary number has a length L of 13, the resultant decimal number has four digits, and a preset value greater than 999 and smaller than 1807 is added to the resultant decimal number.

26. (New) The method of claim 25, wherein a set of numbers 0 through 8191 is allocated to n_5 subsets M_1, \dots, M_{n_5} , and a preset value d_i is added to the resultant decimal number if it is an element of the set M_i , where $999 < d_1 < d_2 < \dots < d_{n_5} < 1809$ and n_5 is a natural number.

27. (New) The method of claim 24, wherein the binary number has a length L of 16, the resultant decimal number has five digits, and a preset value greater than 9999 and smaller than 34465 is added to the resultant decimal number.

28. (New) The method of claim 27, wherein a set of numbers 0 through 65535 is allocated to n_5 subsets M_1, \dots, M_{n_5} , and a preset value d_i is added to the resultant decimal number if it is an element of the set M_i , where $9999 < d_1 < d_2 < \dots < d_{n_5} < 34465$ and n_5 is a natural number.

29. (New) The method of claim 18, wherein:

a first digit of the personal identification number is generated by:

generating a pseudo-random number composed of up to 36

hexadecimal digits from a binary number of a length L ;

converting each hexadecimal digit of the pseudo-random number using one different one out of 36 possible different mathematical mappings of the 36 hexadecimal digits into digits 1 through 9, into another digit of the digits 1 through 9, forming a generated number;

linking up to 36 decimal digits of a generated number in a mathematical operating to form a decimal digit that is unequal to zero and that represents a first digit of the personal identification number, to average out a probability of a particular personal identification digit occurring; and a second digit and each following digit of the personal identification number is generated by:

generating another pseudo-random number composed of up to 210 hexadecimal digits from the binary number of length L;

converting each hexadecimal digit of the another pseudo-random number into one decimal digit using each time one different one out of a 210 possible mathematical mappings of hexadecimal digits into decimal digits; and

linking up to 210 decimal digits of a generated number in a mathematical operation to form a decimal digit representing a particular digit of the personal identification number, to average out the probability of the particular personal identification digit occurring.

30. (New) The method of claim 29, wherein the first digit of the personal identification number is generated in that the up to 36 digits are linked using a group operation of any arbitrary mathematical group of an order 9, and the second digit and each following digit of the personal identification number are generated in that the up to 210 digits are linked using a group operation of any arbitrary mathematical group of an order 10.

31. (New) The method of claim 30, wherein an additive group of integers modulo 10 are used to link the up to 210 digits.

32. (New) The method of claim 30, wherein a multiplicative group of integers modulo 11 are used to link the up to 210 digits.

33. (New) The method of claim 30, wherein a group of symmetric mappings of at least one of a regular pentagon and a dihedral group is used to link the up to 210 digits, each ten symmetric mappings of the group of symmetric mappings of the at least one of the regular pentagon and the dihedral group being assigned a different decimal digit.

34. (New) The method of claim 33, wherein a digit 0 is assigned to an identity mapping,

digits 1 through 4 are assigned to four rotations about a midpoint of the at least one of the regular pentagon and the dihedral group, and digits 5 through 9 are assigned to five reflections about five axes of symmetry of the at least one of the regular pentagon and the dihedral group.

35. The method of claim 18, wherein the binary number is a binary code specific to an individual.

REMARKS

This Preliminary Amendment cancels without prejudice original claims 1 to 17 in the underlying PCT Application No. PCT/EP00/02481, and adds without prejudice new claims 18 to 35. The new claims conform the claims to U.S. Patent and Trademark Office rules and do not add new matter to the application.

In accordance with 37 C.F.R. § 1.121(b)(3), the Substitute Specification (including the Abstract, but without the claims) contains no new matter. The amendments reflected in the Substitute Specification (including Abstract) are to conform the Specification and Abstract to U.S. Patent and Trademark Office rules or to correct informalities. As required by 37 C.F.R. § 1.121(b)(3)(iii) and § 1.125(b)(2), a Marked Up Version Of The Substitute Specification comparing the Specification of record and the Substitute Specification also accompanies this Preliminary Amendment. In the Marked Up Version, double-underlining indicates added text and bracketing indicates deleted text. Approval and entry of the Substitute Specification (including Abstract) is respectfully requested.

The underlying PCT Application No. PCT/EP00/02481 includes an International Search Report, dated August 30, 2000. The Search Report includes a list of documents that were uncovered in the underlying PCT Application. A copy of the Search Report accompanies this Preliminary Amendment.

The underlying PCT Application No. PCT/EP00/02481 also includes an International Preliminary Examination Report, dated February 26, 2001, and an annex associated with the International Preliminary Examination Report. An English translation of the International Preliminary Examination Report and of the annex accompanies this Preliminary Amendment.

Applicants assert that the subject matter of the present application is new, non-obvious, and useful. Prompt consideration and allowance of the application are respectfully requested.

Dated: 10/1/2001

Respectfully Submitted,
KENYON & KENYON

By: Richard L. Mayer

Richard L. Mayer
(Reg. No. 22,490)

One Broadway
New York, NY 10004
(212) 425-7200 (telephone)
(212) 425-5288 (facsimile)

CUSTOMER NO. 26646

(By Richard L. Mayer)
Reg. No. 22,490
33,885-
Haven C
DEPOSIT

2/PRTS

09/9379-2

[2345/165]

30/12/2001 01:00 01 OCT 2001

METHOD FOR GENERATING IDENTIFICATION NUMBERS

FIELD OF THE INVENTION

The present invention relates to a method for generating a personal identification number (PIN), made up of a number of N decimal digits, to be used for money cards and other devices requiring security, from a binary number having L digits, in particular from a binary code specific to an individual.

BACKGROUND INFORMATION

When using automatic cash dispensers, such as ATM machines or similar devices where a plastic card is utilized, the user must often use a four-digit number (PIN) known only to himself in order to receive authorization. There are, by far, however, not as many different PINs as there are users, which is why each PIN exists many times over.

The PINs may only contain decimal digits, to enable them to be entered using numerical keypads. In addition, they are not supposed to begin with a zero. This means that, given four digit positions, the result is a range of 9000 different PINs. The theoretically lowest probability of correctly guessing a PIN is, thus, 1/9000.

SUMMARY OF THE INVENTION

An exemplary method and/or exemplary embodiment of the present invention is directed to providing a method which will keep the probability of a PIN being correctly guessed as low as possible.

When the PINs are generated such that they are randomly uniformly distributed over the available number domain, the probability of a PIN being correctly ascertained may then become minimal.

Express Mail No. EL 244508 211US

SUBSTITUTE SPECIFICATION

With the aid of an encryption algorithm, a secret key may be used to produce a binary code from personal data pertaining to the user. Using the DES (data encryption standard) or triple DES algorithm provided, for example, for generating PINs for money cards, a 64-digit binary code is generated from the data pertaining to one customer, with the assistance of a bank-specific key. From a 16-digit segment of this binary code, the PIN can be generated in the following manner.

For example, four parts for each of the four digits of this binary number are combined into four decimal numbers. These four decimal numbers are divided by 10 (modulo function) to yield the four digits of the PIN as a remainder of a division. If the first digit is a zero, it is replaced by a one. To a large degree, however, the resultant PINs are unevenly distributed over the available number domain of 1 to 9000. If it begins with a 1, a PIN generated in this manner has a probability of being correctly guessed of even greater than 1/150.

If, on the other hand, the PINs are distributed uniformly over the number domain, then the rate of occurrence of each PIN is constantly 1/9000, and the probability of it being correctly guessed is, therefore, also minimal.

Another exemplary embodiment and/or exemplary method of the present invention provides for the first n_1 digits of the binary number (B) to be converted in an available manner into a decimal number d_1 , the predefinable natural number n_1 being selected so as to yield a natural number z_1 such that the quotient $2^{n_1}/(z_1 \cdot 9)$ is close to 1; and for the first decimal digit of the PIN to receive the value d_1 modulo 9; for $N-1$ further groups of further n_2 digits of the binary number (B) to be converted each time in an available manner into $N-1$ decimal numbers d_2 through d_N , the predefinable number n_2 being selected so as to yield a natural number z_2 such that

the quotient $2^{n2}/(z2*10)$ is close to 1, to satisfy the condition: $0 \leq 2^{n2} \text{ modulo } 10 < 3$; and for the decimal digits 2 through N of the PIN to receive the values $d_i \text{ modulo } 10$, $i=2$ through N.

5 To generate the first digit of the PIN, $n1$ is selected so that 2^{n1} is close to a multiple of 9. The $n-1$ digit part to the front of the binary number is interpreted as a decimal number. The integer remainder is calculated by dividing by 9. This remainder forms the first digit of the PIN. To generate digit
10 2 and the following digits of the PIN, $n2$ bits are split off each time. The number $n2$ is selected such that 2^n is close to a multiple of 10. The resulting number is interpreted as a decimal number. The integer remainder is calculated by dividing by 10. This remainder forms the respective digit of
15 the PIN. It is true that no absolute uniform distribution is derived hereby. However, the greater $n2$ is, the more uniformly the PIN numbers are distributed.

For example, selecting $n2=13$ results in a number domain of
20 from 1 to $2^{13}=8192$. The digits 0, 1, 2 and 3 occur in the generated PINs with a probability of $820/8192$, and the remaining digits with a probability of $819/8192$. The exemplary embodiments and/or exemplary methods of the present invention may avoid having the 1 occur all too often in the first digit
25 position of the PIN.

A further exemplary embodiment and/or exemplary method of the present invention is directed to providing for $n1$ and $n2 \leq 16$ to be predefined.

30 A further exemplary embodiment and/or exemplary method of the present invention is directed to providing for $N=4$ to be selected.

A further exemplary embodiment and/or exemplary method of the present invention is directed to providing for the binary

number (B) to have the length $L=16$, for $N=4$ to be predefined, and for $n_1=n_2=4$ to be predefined.

A further exemplary embodiment and/or exemplary method of the present invention is directed to providing for the binary number (B) to have the length $L=3*n_3$, for n_3 groups of three digits of the binary number (B) to be converted in an available manner into n_3 decimal digits to generate the digits of the PIN, n_3 being a natural number. In this variant, altogether 12 bits of the customer-specific binary code are used to generate the PIN. In each case, three bits of this binary number are interpreted as decimal digits between 1 and 8. The PINs produced in this manner are absolutely uniformly distributed.

Another exemplary embodiment and/or exemplary method for generating absolutely uniformly distributed PINs within the particular number domain provides for the binary number to be completely converted into a decimal number, in order to generate the PIN in an available manner, and, if necessary, to add a correction value to the resultant decimal number such that the first digit of the decimal number becomes unequal to zero, the digits of the result forming the digits of the PIN.

To this end, it may be provided for the binary number to have a length L of 13, for the generated decimal number to have four digits, and for a preset value greater than 999 and smaller than 1807 to be added to the decimal number; for the binary number to have a length L of 16, for the generated decimal number to have five digit positions, and for a preset value greater than 9999 and smaller than 34465 to be added to the decimal number.

Furthermore, it may be provided in the first case ($L=13$) for the set of numbers 0 through 8191 to be allocated to n_5 subsets M_1, \dots, M_{n_5} , and for a preset value d_i to be added to the generated decimal number if it is an element of the set

Mi, it holding that $999 < d_1 < d_2 < \dots < d_{n5} < 1809$, and n_5 being a natural number.

Furthermore, it may be provided in the second case ($L=16$) for the set of numbers 0 through 65535 to be allocated to n_5 subsets M_1, \dots, M_{n5} , and for a preset value d_i to be added to the generated decimal number if it is an element of the set M_i , it holding that $9999 < d_1 < d_2 < \dots < d_{n5} < 34465$, and n_5 being a natural number.

Another exemplary embodiment and/or exemplary method of the present invention provides for executing the following steps to generate the first digits of the PIN:

- a pseudo-random number composed of up to 36 hexadecimal digits is generated from the binary number (B) of length L;
- each hexadecimal digit of this number is converted using one different one out of the 36 possible mathematical mappings of hexadecimal digits into the digits 1 through 9, into a digit of the digits 1 through 9;
- to even out the probability of the particular PIN digit occurring, the up to 36 decimal digits of the thus generated number are linked or associated in a mathematical operation to form a decimal digit unequal to zero, which represents the first digit of the PIN;

and for the following steps to be executed for the second and each following digit of the PIN to be generated:

- a pseudo-random number composed of up to 210 hexadecimal digits is generated from the binary number (B) of length L;
- each hexadecimal digit of this number is converted into one decimal digit using each time one different one out of the 210 possible mathematical mappings of hexadecimal digits into decimal digits;
- to average out the probability of the particular PIN digit occurring, the up to 210 decimal digits of the thus generated number are linked in a mathematical operation to form a decimal digit, which represents the particular digit of the PIN;

In another exemplary embodiment and/or exemplary method, the first digit of the PIN may be generated so that the up to 36 digits are linked using the group operation of any arbitrary mathematical group of the order 9, and that the second and the following digits of the PIN are generated, so that the up to 210 digits are linked using the group operation of any arbitrary mathematical group of the order 10.

In this exemplary embodiment and/or exemplary method of the present invention, one hexadecimal number each is generated from N groups of 4 bit length each. It is intended at this point to convert it into a decimal digit. Altogether $(10 \text{ over } 6) = (10 \text{ over } 4) = 210$ different mappings of the hexadecimal digits into the set of decimal digits are available for this conversion. One possible mapping is forming the remainder in a division operation by 10: (0 -> 0, 1 -> 1, 2 -> 2, 3 -> 3, 4 -> 4, 5 -> 5, 6 -> 6, 7 -> 7, 8 -> 8, 9 -> 9, A -> 0, B -> 1, C -> 2, D -> 3, E -> 4, F -> 5). Following this mapping operation, the digits 0 to 5 occur with the rate of occurrence of 1/8, and the digits from 6 to 9 with the rate of occurrence of 1/16. At this point, in order to obtain digits whose probability of occurrence does not deviate or deviates imperceptibly from 1/10, it is proposed to convert the 210 hexadecimal digits, which were generated, for example, by applying the above-mentioned DES algorithm 14 times to the 64-digit binary initial number, (therefore, pseudo-random number, since the generated number is in no way randomly formed), using one each of the other 210 possible mappings, into a decimal digit and, subsequently, linking all 210 decimal digits to one single digit using a group operation of a mathematical group having ten elements. The probability of occurrence of each of the thus generated decimal digits is close to 1/10.

Another exemplary embodiment and/or exemplary method of the present invention is directed to providing for the additive

group of the integers modulo 10 to be used to link the up to 210 digits. In this context, 210 decimal digits are linked to form one single digit, in that one adds all digits and takes as a result, the remainder of a division of the sum by 10. The ten possible results that occur in the process constitute the elements of the additive group $Z_{10,+}$.

Another exemplary embodiment and/or exemplary method of the present invention provides for using the multiplicative group of the integers modulo 11 for linking the up to 210 digits. This group Z_{11}^* likewise has ten elements and is, therefore, suited for linking the numbers to a decimal digit. In Z_{11}^* , one calculates by multiplying two elements and dividing the result by 11. The remaining remainder forms the result of the operation. The zero is removed from the group. The 0 occurring in the digits indexes element no. 10 of the group Z_{11}^* .

Another exemplary embodiment and/or exemplary method of the present invention is directed to providing that the group of the symmetric mappings of a regular pentagon (dihedral group) be used for linking the up to 210 digits, each of the ten symmetric mappings of this group being assigned a different decimal digit. To this end, it may also be provided for the digit 0 to be assigned to the identity mapping, digits 1 through 4 to be assigned the four rotations about the midpoint of the pentagon, digits 5 through 9 to be assigned to the five reflections about the five axes of symmetry of the pentagon. If one executes two symmetric mappings one after another, then a symmetric mapping again results. Based on these allocations, one can set up the following multiplication table:

*	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	2	3	4	0	6	7	8	9	5
2	2	3	4	0	1	7	8	9	5	6
3	3	4	0	1	2	8	9	5	6	7
4	4	0	1	2	3	9	5	6	7	8
5	5	9	8	7	6	0	4	3	2	1

6	6	5	9	8	7	1	0	4	3	2
7	7	6	5	9	8	2	1	0	4	3
8	8	7	6	5	9	3	2	1	0	4
9	9	8	7	6	5	4	3	2	1	0.

5

With the assistance of this table, the 210 digits are linked to one single digit in that, utilizing the result from the previous operation as a row indicator and utilizing the next digit as a column indicator, the next result in the table is read off successively until all digits are considered. The last result forms the desired digit of the PIN.

10

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 shows a diagram for generating a customer-specific binary code.

15

Figure 2 shows a diagram for generating a PIN through conversion to a decimal number.

20

Figure 3 shows a diagram for generating a PIN by a digit-by-digit conversion into decimal numbers.

Figure 4 shows a diagram for generating a PIN by a digit-by-digit conversion, including modulus formation.

25

Figure 5 shows a diagram for generating a PIN by reducing hexadecimal numbers with the assistance of mathematical groups.

DETAILED DESCRIPTION

30

Figure 1 depicts a flow diagram for converting personal data D_c of a customer using a secret key K into a binary number B of L bits length. The binary number B is part of the 64-bit long encryption result, which was generated from the customer data D_c using the DES algorithm.

35

If the length of the binary number B equals 13, and if the number of the PIN digits to be generated equals 4, then the

PIN, as shown in Figure 2, can be generated by interpreting the binary number B as decimal number D by adding a constant C thereto. The constant is to be selected such that the PIN does not have any leading zeros. In this manner, 8192 different
5 PINS can be generated, which are absolutely uniformly distributed over the number domain in question.

Figure 3 depicts how a binary number of length 13 can be converted into a PIN in that for each digit of the PIN to be generated, a number of bits of the binary number is converted
10 into a decimal number, and a constant C is added to the resultant number D, to avoid having leading zeros of the PIN. In this manner, 7777 different PINS may be generated, which are absolutely uniformly distributed over the number domain in question.

Another example for generating nearly equally distributed PINs from a binary number B is illustrated in Figure 4. The binary number B has 52 digit positions. To generate the four-digit PIN, the binary number B is subdivided into four subsets,
15 which, in the example, have the same length. Each of these subsets is interpreted as a decimal number. The first digit of the PIN is derived as a remainder of a division of the first decimal number by 9. The following digits of the PIN are derived in each case as a remainder of a division of the
20 following decimal number by 10. In this manner, 9000 different PINS may be generated, which are absolutely uniformly distributed.

From the personal data Dc of a customer, as shown in Figure 5, a sequence of 210 hexadecimal digits is generated with the
30 assistance of a secret key and a random-number generator, in that, for example, an encryption result of the DES algorithm from Figure 1 is again encrypted using the algorithm, and so forth. The 14 64-digit binary codes resulting therefrom are converted into 14 hexadecimal numbers Hi, each having 16

digits. Lined up, this yields 224 hexadecimal digits, of which 210 enter into the generation of the PIN.

There are 210 different possibilities f_i for mapping the set of 16 hexadecimal digits into the set of the 10 decimal digits. Therefore, each of the 210 hexadecimal digits is converted using a different one of these mappings into a decimal digit d_i . In order to produce a digit Z_i of a PIN from the 210 decimal digits, they are successively linked using the group operation F of any arbitrary ten-element mathematical group; the last result is the sought after digit. Thus, the previously non-uniform, statistical distribution of the 210 decimal digits is evened out. The entire process is repeated for each of the digit positions Z_2 through Z_4 of the PIN.

Analogously for the first digit of the PIN, 36 hexadecimal digits are generated, which are mapped with every other one of the 36 possible mappings of the hexadecimal digits into the set of the digits 1 through 9, into a digit between 1 and 9. The 36 decimal digits are linked to the first digit of the PIN using the group operation of any arbitrary mathematical group of the order 9. This enables 9000 different PINs to be generated which are nearly uniformly distributed. In generating 10^5 PINs, the maximum non-uniformities amounted to about 1.5 percent. This does not significantly raise the probability of a PIN being accidentally correctly guessed as compared to the theoretical minimum value. Thus, the method functions very reliably.

All mathematical groups having ten elements are fundamentally suited for use with this method. Known representatives include the additive group of the integers modulo 10, $Z_{10,+}$, the multiplicative group of the integers modulo 11, Z_{11}^* , as well as the group of the symmetric mapping(s) of a regular pentagon D_5 , the so-called dihedral group. In the last instance, one decimal digit, which may be used for the calculation, is assigned to each of the individual elements of the group.

ABSTRACT OF THE DISCLOSURE

A method for generating a personal identification number (PIN), made up of a number of N decimal digits, to be used for money cards and other devices requiring security, from a binary number having L digits, in particular from a binary code specific to an individual, the PINs are generated such that they are randomly uniformly distributed over the available number domain.

5

2/PATS

09/937923

JC12 Rec'd PCT/PTO 01 OCT 2001

[2345/165]

[]

METHOD FOR GENERATING IDENTIFICATION NUMBERS

FIELD OF THE INVENTION

The present invention [is directed]relates to a method for generating a personal identification number (PIN), made up of a number of N decimal digits, to be used for money cards and other devices requiring security, from a binary number having L digits, in[] particular from a binary code specific to an individual.

BACKGROUND INFORMATION

When using automatic cash dispensers, such as ATM machines or similar devices where a plastic card is utilized, the user must often use a four-digit number (PIN) known only to himself in order to receive authorization. There are, by far, however, not as many different PINs as there are users, which is why each PIN exists many times over.[]

The PINs may only contain decimal digits, to enable them to be entered using numerical keypads. In addition, they are not supposed to begin with a zero. This means that, given four digit positions, the result is a range of 9000 different PINs. The theoretically lowest probability of correctly guessing a PIN is, thus, 1/9000.

[The object]SUMMARY OF THE INVENTION

An exemplary method and/or exemplary embodiment of the present invention is directed to [provide]providing a method which will keep the probability of a PIN being correctly guessed as low as possible.[]

[The realization underlying the present invention is that w]When the PINs are generated such that they are randomly

MARKED UP VERSION OF THE SUBSTITUTE SPECIFICATION

NY01 411329 v 1

Express Mail No. EL244509211US

uniformly distributed over the available number domain, the probability of a PIN being correctly ascertained may then become[s] minimal. [This is elucidated on the basis of the following example.]

5

With the aid of an encryption algorithm, a secret key may be used to produce a binary code from personal data pertaining to the user. Using the DES (data encryption standard) or triple DES algorithm provided, for example, for generating PINs for
10 money cards, a 64-digit binary code is generated from the data pertaining to one customer, with the assistance of a bank-specific key. From a 16-digit segment of this binary code, the PIN can be generated in the following manner[, for].

15 For example[:

Four], four parts for each of the four digits of this binary number are combined into four decimal numbers. These four decimal numbers are divided by 10 (modulo function) to yield
20 the four digits of the PIN as a remainder of a division. If the first digit is a zero, it is replaced by a one. To a large degree, however, the resultant PINs are unevenly distributed over the available number domain of 1 to 9000. If it begins with a 1, a PIN generated in this manner has a probability of
25 being correctly guessed of even greater than 1/150.

If, on the other hand, [one distributes the PINs] the PINs are distributed uniformly over the number domain, then the rate of occurrence of each PIN is constantly 1/9000, and the
30 probability of it being correctly guessed is, therefore, also minimal.

[A first] Another exemplary embodiment and/or exemplary method of the present invention provides for the first n1 digits of
35 the binary number (B) to be converted in [generally known fashion] an available manner into a decimal number d1, the

predefinable natural number n_1 being selected so as to yield a natural number z_1 such that the quotient $2^{n_1}/(z_1*9)$ is close to 1; and for the first decimal digit of the PIN to receive the value d_1 modulo 9; for $N-1$ further groups of further n_2 digits of the binary number (B) to be converted each time in [generally known fashion]an available manner into $N-1$ decimal numbers d_2 through d_N , the predefinable number n_2 being selected so as to yield a natural number z_2 such that the quotient $2^{n_2}/(z_2*10)$ is close to 1, [the intention being] to satisfy the condition: $0 \leq 2^{n_2} \text{ modulo } 10 < 3$; and for the decimal digits 2 through N of the PIN to receive the values d_i modulo 10, $i=2$ through N .

To generate the first digit of the PIN, n_1 is selected so that 2^{n_1} is close to a multiple of 9. The $n-1$ digit part to the front of the binary number is interpreted as a decimal number. The integer remainder is calculated by dividing by 9. This remainder forms the first digit of the PIN. To generate digit 2 and the following digits of the PIN, n_2 bits are split off each time. The number n_2 is selected such that 2^n is close to a multiple of 10. The resulting number is interpreted as a decimal number. The integer remainder is calculated by dividing by 10. This remainder forms the respective digit of the PIN. It is true that no absolute uniform distribution is derived hereby. However, the greater n_2 is, the more uniformly the PIN numbers are distributed.

For example, selecting $n_2=13$ results in a number domain of from 1 to $2^{13}=8192$. The digits 0, 1, 2 and 3 occur in the generated PINs with a probability of $820/8192$, and the remaining digits with a probability of $819/8192$. [In particular, the]The exemplary embodiments and/or exemplary methods of the present invention may avoid[s] having the 1 occur all too often in the first digit position of the PIN.

A further exemplary embodiment and/or exemplary method of the present invention [provides] is directed to providing for n_1 and $n_2 \leq 16$ to be predefined.

5 [Yet another] A further exemplary embodiment and/or exemplary method of the present invention [provides] is directed to providing for $N=4$ to be selected.

10 [Furthermore, it may be provided] A further exemplary embodiment and/or exemplary method of the present invention is directed to providing for the binary number (B) to have the length $L=16$, for $N=4$ to be predefined, and for $n_1=n_2=4$ to be predefined.

15 [Yet another] A further exemplary embodiment and/or exemplary method of the present invention [provides] is directed to providing for the binary number (B) to have the length $L=3 \cdot n_3$, for n_3 groups of three digits of the binary number (B) to be converted in [generally known fashion] an available manner into n_3 decimal digits to generate the digits of the PIN, n_3 being a natural number. In this variant, altogether 12 bits of the customer-specific binary code are used to generate the PIN. In
20 each case, three bits of this binary number are interpreted as decimal digits between 1 and 8. The PINs produced in this manner are absolutely uniformly distributed.

25 Another [possibility] exemplary embodiment and/or exemplary method for generating absolutely uniformly distributed PINs within the particular number domain provides for the binary number to be completely converted into a decimal number, in order to generate the PIN in [generally known fashion] an available manner, and, if necessary, to add a correction value to the resultant decimal number such that the first digit of
30 the decimal number becomes unequal to zero, the digits of the result forming the digits of the PIN.

To this end, it may be provided for the binary number to have a length L of 13, for the generated decimal number to have four digits, and for a preset value greater than 999 and smaller than 1807 to be added to the decimal number; for the
5 binary number to have a length L of 16, for the generated decimal number to have five digit positions, and for a preset value greater than 9999 and smaller than 34465 to be added to the decimal number.

10 Furthermore, it may be provided in the first case (L=13) for the set of numbers 0 through 8191 to be allocated to n5 subsets M1,...,Mn5, and for a preset value di to be added to the generated decimal number if it is an element of the set Mi, it holding that $999 < d1 < d2 < \dots < dn5 < 1809$, and n5 being a
15 natural number.

Furthermore, it may be provided in the second case (L=16) for the set of numbers 0 through 65535 to be allocated to n5 subsets M1,...,Mn5, and for a preset value di to be added to the generated decimal number if it is an element of the set
20 Mi, it holding that $9999 < d1 < d2 < \dots < dn5 < 34465$, and n5 being a natural number.

Another exemplary embodiment and/or exemplary method of the present invention provides for executing the following steps to generate the first digits of the PIN:

- 25 - a pseudo-random number composed of up to 36 hexadecimal digits is generated from the binary number (B) of length L;
- each hexadecimal digit of this number is converted using one different one out of the 36 possible mathematical mappings of hexadecimal digits into the digits 1 through 9, into a
30 digit of the digits 1 through 9;
- to even out the probability of the particular PIN digit occurring, the up to 36 decimal digits of the thus generated number are linked or associated in a mathematical operation

to form a decimal digit unequal to zero, which represents the first digit of the PIN;
and for the following steps to be executed for the second and each following digit of the PIN to be generated:

- a pseudo-random number composed of up to 210 hexadecimal digits is generated from the binary number (B) of length L;
- each hexadecimal digit of this number is converted into one decimal digit using each time one different one out of the 210 possible mathematical mappings of hexadecimal digits into decimal digits;
- to average out the probability of the particular PIN digit occurring, the up to 210 decimal digits of the thus generated number are linked in a mathematical operation to form a decimal digit, which represents the particular digit of the PIN;

[For this purpose]In another exemplary embodiment and/or exemplary method, [it may be provided that] the first digit of the PIN ismay be generated inso that the up to 36 digits are linked using the group operation of any arbitrary mathematical group of the order 9, and that the second and the following digits of the PIN are generated, inso that the up to 210 digits are linked using the group operation of any arbitrary mathematical group of the order 10.

In this exemplary embodiment [of the]and/or exemplary method of the present invention, one hexadecimal number each is generated from N groups of 4 bit length each. It is intended at this point to convert it into a decimal digit. Altogether $(10 \text{ over } 6) = (10 \text{ over } 4) = 210$ different mappings of the hexadecimal digits into the set of decimal digits are available for this conversion. One possible mapping is forming the remainder in a division operation by 10: (0 -> 0, 1 -> 1, 2 -> 2, 3 -> 3, 4 -> 4, 5 -> 5, 6 -> 6, 7 -> 7, 8 -> 8, 9 -> 9, A -> 0, B -> 1, C -> 2, D -> 3, E -> 4, F -> 5). Following this mapping operation, the digits 0 to 5 occur with the rate

of occurrence of 1/8, and the digits from 6 to 9 with the rate of occurrence of 1/16. At this point, in order to obtain digits whose probability of occurrence does not deviate or deviates imperceptibly from 1/10, it is proposed to convert the 210 hexadecimal digits, which were generated, for example, by applying the above-mentioned DES algorithm 14 times to the 64-digit binary initial number, (therefore, pseudo-random number, since the generated number is in no way randomly formed), using one each of the other 210 possible mappings, into a decimal digit and, subsequently, linking all 210 decimal digits to one single digit using a group operation of a mathematical group having ten elements. The probability of occurrence of each of the thus generated decimal digits is close to 1/10.

[A next] Another exemplary embodiment and/or exemplary method of the present invention [provides] is directed to providing for the additive group of the integers modulo 10 to be used to link the up to 210 digits. In this context, 210 decimal digits are linked to form one single digit, in that one adds all digits and takes as a result, the remainder of a division of the sum by 10. The ten possible results that occur in the process constitute the elements of the additive group $Z_{10,+}$.

Another exemplary embodiment and/or exemplary method of the present invention provides for using the multiplicative group of the integers modulo 11 for linking the up to 210 digits. This group Z_{11}^* likewise has ten elements and is, therefore, suited for linking the numbers to a decimal digit. In Z_{11}^* , one calculates by multiplying two elements and dividing the result by 11. The remaining remainder forms the result of the operation. The zero is removed from the group. The 0 occurring in the digits indexes element no. 10 of the group Z_{11}^* .

Another exemplary embodiment and/or exemplary method of the present invention [provides] is directed to providing that the group of the symmetric mappings of a regular pentagon

(dihedral group) be used for linking the up to 210 digits, each of the ten symmetric mappings of this group being assigned a different decimal digit. To this end, it may also be provided for the digit 0 to be assigned to the identity mapping, digits 1 through 4 to be assigned the four rotations about the midpoint of the pentagon, digits 5 through 9 to be assigned to the five reflections about the five axes of symmetry of the pentagon. If one executes two symmetric mappings one after another, then a symmetric mapping again results. Based on these allocations, one can set up the following multiplication table:

* 0 1 2 3 4 5 6 7 8 9	
0	0 1 2 3 4 5 6 7 8 9
1	1 2 3 4 0 6 7 8 9 5
2	2 3 4 0 1 7 8 9 5 6
3	3 4 0 1 2 8 9 5 6 7
4	4 0 1 2 3 9 5 6 7 8
5	5 9 8 7 6 0 4 3 2 1
6	6 5 9 8 7 1 0 4 3 2
7	7 6 5 9 8 2 1 0 4 3
8	8 7 6 5 9 3 2 1 0 4
9	9 8 7 6 5 4 3 2 1 0.

With the assistance of this table, the 210 digits are linked to one single digit in that, utilizing the result from the previous operation as a row indicator and utilizing the next digit as a column indicator, the next result in the table is read off successively until all digits are considered. The last result forms the desired digit of the PIN.

[Exemplary embodiments of the present invention are represented by several figures in the drawing and are elucidated in the following description. The figures show:

Figure 1]BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 shows a diagram for generating a customer-specific binary code[;

] .

Figure 2[] shows a diagram for generating a PIN through
conversion to a decimal number[;].

Figure 3[] shows a diagram for generating a PIN by a digit-
by-digit conversion into decimal numbers[;
]..

Figure 4[] shows a diagram for generating a PIN by a digit-
by-digit conversion, including modulus formation[;
and
]..

Figure 5[] shows a diagram for generating a PIN by reducing
hexadecimal numbers with the assistance of
mathematical groups.[

Identical or corresponding parts are provided with the same
reference numerals in the figures.

]

DETAILED DESCRIPTION

Figure 1 depicts a flow diagram for converting personal data
Dc of a customer using a secret key K into a binary number B
of L bits length. The binary number B is part of the 64-bit
long encryption result, which was generated from the customer
data Dc using the DES algorithm.[

]

If the length of the binary number B equals 13, and if the
number of the PIN digits to be generated equals 4, then the
PIN, as shown in Figure 2, can be generated by interpreting
the binary number B as decimal number D by adding a constant C
thereto. The constant is to be selected such that the PIN does
not have any leading zeros. In this manner, 8192 different
PINS can be generated, which are absolutely uniformly
distributed over the number domain in question.

Figure 3 depicts how a binary number of length 13 can be converted into a PIN in that for each digit of the PIN to be generated, a number of bits of the binary number is converted into a decimal number, and a constant C is added to the resultant number D, to avoid having leading zeros of the PIN. In this manner, 7777 different PINS may be generated, which are absolutely uniformly distributed over the number domain in question.

Another [possibility]example for generating nearly equally distributed PINs from a binary number B is illustrated in Figure 4. The binary number B has 52 digit positions. To generate the four-digit PIN, the binary number B is subdivided into four subsets, which, in the example, have the same length. Each of these subsets is interpreted as a decimal number. The first digit of the PIN is derived as a remainder of a division of the first decimal number by 9. The following digits of the PIN are derived in each case as a remainder of a division of the following decimal number by 10. In this manner, 9000 different PINS may be generated, which are absolutely uniformly distributed.

From the personal data D_c of a customer, as shown in Figure 5, a sequence of 210 hexadecimal digits is generated with the assistance of a secret key and a random-number generator, in that, for example, an encryption result of the DES algorithm from Figure 1 is again encrypted using the algorithm, and so forth. The 14 64-digit binary codes resulting therefrom are converted into 14 hexadecimal numbers H_i , each having 16 digits. Lined up, this yields 224 hexadecimal digits, of which 210 enter into the generation of the PIN.

There are 210 different possibilities f_i for mapping the set of 16 hexadecimal digits into the set of the 10 decimal digits. Therefore, each of the 210 hexadecimal digits is converted using a different one of these mappings into a

decimal digit d_i . In order to produce a digit Z_i of a PIN from the 210 decimal digits, they are successively linked using the group operation F of any arbitrary ten-element mathematical group; the last result is the sought after digit. Thus, the previously non-uniform, statistical distribution of the 210 decimal digits is evened out. The entire process is repeated for each of the digit positions Z_2 through Z_4 of the PIN.

Analogously for the first digit of the PIN, 36 hexadecimal digits are generated, which are mapped with every other one of the 36 possible mappings of the hexadecimal digits into the set of the digits 1 through 9, into a digit between 1 and 9. The 36 decimal digits are linked to the first digit of the PIN using the group operation of any arbitrary mathematical group of the order 9. This enables 9000 different PINs to be generated which are nearly uniformly distributed. In generating 10^5 PINs, the maximum non-uniformities amounted to about 1.5 percent. This does not significantly raise the probability of a PIN being accidentally correctly guessed as compared to the theoretical minimum value. Thus, the method functions very reliably.

All mathematical groups having ten elements are fundamentally suited for use with this method. Known representatives include the additive group of the integers modulo 10, $Z_{10,+}$, the multiplicative group of the integers modulo 11, Z_{11}^* , as well as the group of the symmetric [mappings]mapping(s) of a regular pentagon D_5 , the so-called dihedral group. In the last instance, one decimal digit, which may be used for the calculation, is assigned to each of the individual elements of the group.

[

Abstract

]

ABSTRACT OF THE DISCLOSURE

[In a] A method for generating a personal identification number (PIN), made up of a number of N decimal digits, to be used for money cards and other devices requiring security, from a binary number having L digits, in particular from a binary code specific to an individual, the PINs are generated such that they are randomly uniformly distributed over the available number domain.

11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1089
1090
1091
1092
1093
1094
1095
1096
1097
1098
1099
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1110
1111
1112
1113
1114
1115
1116
1117
1118
1119
1120
1121
1122
1123
1124
1125
1126
1127
1128
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1140
1141
1142
1143
1144
1145
1146
1147
1148
1149
1150
1151
1152
1153
1154
1155
1156
1157
1158
1159
1160
1161
1162
1163
1164
1165
1166
1167
1168
1169
1170
1171
1172
1173
1174
1175
1176
1177
1178
1179
1180
1181
1182
1183
1184
1185
1186
1187
1188
1189
1190
1191
1192
1193
1194
1195
1196
1197
1198
1199
1200
1201
1202
1203
1204
1205
1206
1207
1208
1209
1210
1211
1212
1213
1214
1215
1216
1217
1218
1219
1220
1221
1222
1223
1224
1225
1226
1227
1228
1229
1230
1231
1232
1233
1234
1235
1236
1237
1238
1239
1240
1241
1242
1243
1244
1245
1246
1247
1248
1249
1250
1251
1252
1253
1254
1255
1256
1257
1258
1259
1260
1261
1262
1263
1264
1265
1266
1267
1268
1269
1270
1271
1272
1273
1274
1275
1276
1277
1278
1279
1280
1281
1282
1283
1284
1285
1286
1287
1288
1289
1290
1291
1292
1293
1294
1295
1296
1297
1298
1299
1300
1301
1302
1303
1304
1305
1306
1307
1308
1309
1310
1311
1312
1313
1314
1315
1316
1317
1318
1319
1320
1321
1322
1323
1324
1325
1326
1327
1328
1329
1330
1331
1332
1333
1334
1335
1336
1337
1338
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1349
1350
1351
1352
1353
1354
1355
1356
1357
1358
1359
1360
1361
1362
1363
1364
1365
1366
1367
1368
1369
1370
1371
1372
1373
1374
1375
1376
1377
1378
1379
1380
1381
1382
1383
1384
1385
1386
1387
1388
1389
1390
1391
1392
1393
1394
1395
1396
1397
1398
1399
1400
1401
1402
1403
1404
1405
1406
1407
1408
1409
1410
1411
1412
1413
1414
1415
1416
1417
1418
1419
1420
1421
1422
1423
1424
1425
1426
1427
1428
1429
1430
1431
1432
1433
1434
1435
1436
1437
1438
1439
1440
1441
1442
1443
1444
1445
1446
1447
1448
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458
1459
1460
1461
1462
1463
1464
1465
1466
1467
1468
1469
1470
1471
1472
1473
1474
1475
1476
1477
1478
1479
1480
1481
1482
1483
1484
1485
1486
1487
1488
1489
1490
1491
1492
1493
1494
1495
1496
1497
1498
1499
1500
1501
1502
1503
1504
1505
1506
1507
1508
1509
1510
1511
1512
1513
1514
1515
1516
1517
1518
1519
1520
1521
1522
1523
1524
1525
1526
1527
1528
1529
1530
1531
1532
1533
1534
1535
1536
1537
1538
1539
1540
1541
1542
1543
1544
1545
1546
1547
1548
1549
1550
1551
1552
1553
1554
1555
1556
1557
1558
1559
1560
1561
1562
1563
1564
1565
1566
1567
1568
1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1589
1590
1591
1592
1593
1594
1595
1596
1597
1598
1599
1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1610
1611
1612
1613
1614
1615
1616
1617
1618
1619
1620
1621
1622
1623
1624
1625
1626
1627
1628
1629
1630
1631
1632
1633
1634
1635
1636
1637
1638
1639
1640
1641
1642
1643
1644
1645
1646
1647
1648
1649
1650
1651
1652
1653
1654
1655
1656
1657
1658
1659
1660
1661
1662
1663
1664
1665
1666
1667
1668
1669
1670
1671
1672
1673
1674
1675
1676
1677
1678
1679
1680
1681
1682
1683
1684
1685
1686
1687
1688
1689
1690
1691
1692
1693
1694
1695
1696
1697
1698
1699
1700
1701
1702
1703
1704
1705
1706
1707
1708
1709
1710
1711
1712
1713
1714
1715
1716
1717
1718
1719
1720
1721
1722
1723
1724
1725
1726
1727
1728
1729
1730
1731
1732
1733
1734
1735
1736
1737
1738
1739
1740
1741
1742
1743
1744
1745
1746
1747
1748
1749
1750
1751
1752
1753
1754
1755
1756
1757
1758
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1769
1770
1771
1772
1773
1774
1775
1776
1777
1778
1779
1780
1781
1782
1783
1784
1785
1786
1787
1788
1789
1790
1791
1792
1793
1794
1795
1796
1797
1798
1799
1800
1801
1802
1803
1804
1805
1806
1807
1808
1809
1810
1811
1812
1813
1814
1815
1816
1817
1818
1819
1820
1821
1822
1823
1824
1825
1826
1827
1828
1829
1830
1831
1832
1833
1834
1835
1836
1837
1838
1839
1840
1841
1842
1843
1844
1845
1846
1847
1848
1849
1850
1851
1852
1853
1854
1855
1856
1857
1858
1859
1860
1861
1862
1863
1864
1865
1866
1867
1868
1869
1870
1871
1872
1873
1874
1875
1876
1877
1878
1879
1880
1881
1882
1883
1884
1885
1886
1887
1888
1889
1890
1891
1892
1893
1894
1895
1896
1897
1898
1899
1900
1901
1902
1903
1904
1905
1906
1907
1908
1909
1910
1911
1912
1913
1914
1915
1916
1917
1918
1919
1920
1921
1922
1923
1924
1925
1926
1927
1928
1929
1930
1931
1932
1933
1934
1935
1936
1937
1938
1939
1940
1941
1942
1943
1944
1945
1946
1947
1948
1949
1950
1951
1952
1953
1954
1955
1956
1957
1958
1959
1960
1961
1962
1963
1964
1965
1966
1967
1968
1969
1970
1971
1972
1973
1974
1975
1976
1977
1978
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2030
2031
2032
2033
2034
2035
2036
2037
2038
2039
2040
2041
2042
2043
2044
2045
2046
2047
2048
2049
2050
2051
2052
2053
2054
2055
2056
2057
2058
2059
2060
2061
2062
2063
2064
2065
2066
2067
2068
2069
2070
2071
2072
2073
2074
2075
2076
2077
2078
2079
2080
2081
2082
2083
2084
2085
2086
2087
2088
2089
2090
2091
2092
2093
2094
2095
2096
2097
2098
2099
2100
2101
2102
2103
2104
2105
2106
2107
2108
2109
2110
2111
2112
2113
2114
2115
2116
2117
2118
2119
2120
2121
2122
2123
2124
2125
2126
2127
2128
2129
2130
2131
2132
2133
2134
2135
2136
2137
2138
2139
2140
2141
2142
2143
2144
2145
2146
2147
2148
2149
2150
2151
2152
2153
2154
2155
2156
2157
2158
2159
2160
2161
2162
2163
2164
2165
2166
2167
2168
2169
2170
2171
2172
2173
2174
2175
2176
2177
2178
2179
2180
2181
2182
2183
2184
2185
2186
2187
2188
2189
2190
2191
2192
2193
2194
2195
2196
2197
2198
2199
2200
2201
2202
2203
2204
2205
2206
2207
2208
2209
2210
2211
2212
2

2/PATS

09/937923

JCO9 Rec'd PCT/PTO 01 OCT 2001

[2345/165]

METHOD FOR GENERATING IDENTIFICATION NUMBERS

The present invention is directed to a method for generating a personal identification number (PIN), made up of a number of N decimal digits, to be used for money cards and other devices requiring security, from a binary number having L digits, in particular from a binary code specific to an individual.

When using automatic cash dispensers, such as ATM machines or similar devices where a plastic card is utilized, the user must often use a four-digit number (PIN) known only to himself in order to receive authorization. There are, by far, however, not as many different PINs as there are users, which is why each PIN exists many times over.

The PINs may only contain decimal digits, to enable them to be entered using numerical keypads. In addition, they are not supposed to begin with a zero. This means that, given four digit positions, the result is a range of 9000 different PINs. The theoretically lowest probability of correctly guessing a PIN is, thus, 1/9000.

The object of the present invention is to provide a method which will keep the probability of a PIN being correctly guessed as low as possible.

The realization underlying the present invention is that when the PINs are generated such that they are randomly uniformly distributed over the available number domain, the probability of a PIN being correctly ascertained becomes minimal. This is elucidated on the basis of the following example.

With the aid of an encryption algorithm, a secret key may be used to produce a binary code from personal data pertaining to the user. Using the DES or triple DES algorithm provided, for example, for generating PINs for money cards, a 64-digit

binary code is generated from the data pertaining to one customer, with the assistance of a bank-specific key. From a 16-digit segment of this binary code, the PIN can be generated in the following manner, for example:

5

Four parts for each of the four digits of this binary number are combined into four decimal numbers. These four decimal numbers are divided by 10 (modulo function) to yield the four digits of the PIN as a remainder of a division. If the first digit is a zero, it is replaced by a one. To a large degree, however, the resultant PINs are unevenly distributed over the available number domain of 1 to 9000. If it begins with a 1, a PIN generated in this manner has a probability of being correctly guessed of even greater than 1/150.

10

15

If, on the other hand, one distributes the PINs uniformly over the number domain, then the rate of occurrence of each PIN is constantly 1/9000, and the probability of it being correctly guessed is, therefore, also minimal.

20

25

30

A first exemplary embodiment of the present invention provides for the first n_1 digits of the binary number (B) to be converted in generally known fashion into a decimal number d_1 , the predefinable natural number n_1 being selected so as to yield a natural number z_1 such that the quotient $2^{n_1}/(z_1 \cdot 9)$ is close to 1; and for the first decimal digit of the PIN to receive the value d_1 modulo 9; for $N-1$ further groups of further n_2 digits of the binary number (B) to be converted each time in generally known fashion into $N-1$ decimal numbers d_2 through d_N , the predefinable number n_2 being selected so as to yield a natural number z_2 such that the quotient $2^{n_2}/(z_2 \cdot 10)$ is close to 1, the intention being to satisfy the condition: $0 \leq 2^{n_2} \text{ modulo } 10 < 3$; and for the decimal digits 2 through N of the PIN to receive the values d_i modulo 10, $i=2$ through N .

35

To generate the first digit of the PIN, n_1 is selected so that 2^{n_1} is close to a multiple of 9. The $n-1$ digit part to the

front of the binary number is interpreted as a decimal number. The integer remainder is calculated by dividing by 9. This remainder forms the first digit of the PIN. To generate digit 2 and the following digits of the PIN, n_2 bits are split off each time. The number n_2 is selected such that 2^{n_2} is close to a multiple of 10. The resulting number is interpreted as a decimal number. The integer remainder is calculated by dividing by 10. This remainder forms the respective digit of the PIN. It is true that no absolute uniform distribution is derived hereby. However, the greater n_2 is, the more uniformly the PIN numbers are distributed.

For example, selecting $n_2=13$ results in a number domain of from 1 to $2^{13}=8192$. The digits 0, 1, 2 and 3 occur in the generated PINs with a probability of $820/8192$, and the remaining digits with a probability of $819/8192$. In particular, the method of the present invention avoids having the 1 occur all too often in the first digit position of the PIN.

A further exemplary embodiment of the present invention provides for n_1 and $n_2 \leq 16$ to be predefined.

Yet another exemplary embodiment of the present invention provides for $N=4$ to be selected.

Furthermore, it may be provided for the binary number (B) to have the length $L=16$, for $N=4$ to be predefined, and for $n_1=n_2=4$ to be predefined.

Yet another exemplary embodiment of the present invention provides for the binary number (B) to have the length $L=3 \cdot n_3$, for n_3 groups of three digits of the binary number (B) to be converted in generally known fashion into n_3 decimal digits to generate the digits of the PIN, n_3 being a natural number. In this variant, altogether 12 bits of the customer-specific binary code are used to generate the PIN. In each case, three bits of this binary number are interpreted as decimal digits

between 1 and 8. The PINs produced in this manner are absolutely uniformly distributed.

Another possibility for generating absolutely uniformly distributed PINs within the particular number domain provides for the binary number to be completely converted into a decimal number, in order to generate the PIN in generally known fashion, and, if necessary, to add a correction value to the resultant decimal number such that the first digit of the decimal number becomes unequal to zero, the digits of the result forming the digits of the PIN.

To this end, it may be provided for the binary number to have a length L of 13, for the generated decimal number to have four digits, and for a preset value greater than 999 and smaller than 1807 to be added to the decimal number; for the binary number to have a length L of 16, for the generated decimal number to have five digit positions, and for a preset value greater than 9999 and smaller than 34465 to be added to the decimal number.

Furthermore, it may be provided in the first case (L=13) for the set of numbers 0 through 8191 to be allocated to n_5 subsets M_1, \dots, M_{n_5} , and for a preset value d_i to be added to the generated decimal number if it is an element of the set M_i , it holding that $999 < d_1 < d_2 < \dots < d_{n_5} < 1809$, and n_5 being a natural number.

Furthermore, it may be provided in the second case (L=16) for the set of numbers 0 through 65535 to be allocated to n_5 subsets M_1, \dots, M_{n_5} , and for a preset value d_i to be added to the generated decimal number if it is an element of the set M_i , it holding that $9999 < d_1 < d_2 < \dots < d_{n_5} < 34465$, and n_5 being a natural number.

Another exemplary embodiment of the present invention provides for executing the following steps to generate the first digits of the PIN:

- a pseudo-random number composed of up to 36 hexadecimal digits is generated from the binary number (B) of length L;
- each hexadecimal digit of this number is converted using one different one out of the 36 possible mathematical mappings of hexadecimal digits into the digits 1 through 9, into a digit of the digits 1 through 9;
- to even out the probability of the particular PIN digit occurring, the up to 36 decimal digits of the thus generated number are linked in a mathematical operation to form a decimal digit unequal to zero, which represents the first digit of the PIN;

and for the following steps to be executed for the second and each following digit of the PIN to be generated:

- a pseudo-random number composed of up to 210 hexadecimal digits is generated from the binary number (B) of length L;
- each hexadecimal digit of this number is converted into one decimal digit using each time one different one out of the 210 possible mathematical mappings of hexadecimal digits into decimal digits;
- to average out the probability of the particular PIN digit occurring, the up to 210 decimal digits of the thus generated number are linked in a mathematical operation to form a decimal digit, which represents the particular digit of the PIN;

For this purpose, it may be provided that the first digit of the PIN is generated in that the up to 36 digits are linked using the group operation of any arbitrary mathematical group of the order 9, and that the second and the following digits of the PIN are generated, in that the up to 210 digits are linked using the group operation of any arbitrary mathematical group of the order 10.

In this exemplary embodiment of the method of the present invention, one hexadecimal number each is generated from N groups of 4 bit length each. It is intended at this point to convert it into a decimal digit. Altogether $(10 \text{ over } 6) = (10$

over 4) = 210 different mappings of the hexadecimal digits into the set of decimal digits are available for this conversion. One possible mapping is forming the remainder in a division by 10: (0 -> 0, 1 -> 1, 2 -> 2, 3 -> 3, 4 -> 4, 5 -> 5, 6 -> 6, 7 -> 7, 8 -> 8, 9 -> 9, A -> 0, B -> 1, C -> 2, D -> 3, E -> 4, F -> 5). Following this mapping operation, the digits 0 to 5 occur with the rate of occurrence of 1/8, and the digits from 6 to 9 with the rate of occurrence of 1/16. At this point, in order to obtain digits whose probability of occurrence does not deviate or deviates imperceptibly from 1/10, it is proposed to convert the 210 hexadecimal digits, which were generated, for example, by applying the above-mentioned DES algorithm 14 times to the 64-digit binary initial number, (therefore, pseudo-random number, since the generated number is in no way randomly formed), using one each of the other 210 possible mappings, into a decimal digit and, subsequently, linking all 210 decimal digits to one single digit using a group operation of a mathematical group having ten elements. The probability of occurrence of each of the thus generated decimal digits is close to 1/10.

A next exemplary embodiment of the present invention provides for the additive group of the integers modulo 10 to be used to link the up to 210 digits. In this context, 210 decimal digits are linked to form one single digit, in that one adds all digits and takes as a result, the remainder of a division of the sum by 10. The ten possible results that occur in the process constitute the elements of the additive group $Z_{10,+}$.

Another exemplary embodiment of the present invention provides for using the multiplicative group of the integers modulo 11 for linking the up to 210 digits. This group Z_{11}^* likewise has ten elements and is, therefore, suited for linking the numbers to a decimal digit. In Z_{11}^* , one calculates by multiplying two elements and dividing the result by 11. The remaining remainder forms the result of the operation. The zero is

removed from the group. The 0 occurring in the digits indexes element no. 10 of the group Z_{11}^* .

Another exemplary embodiment of the present invention provides that the group of the symmetric mappings of a regular pentagon (dihedral group) be used for linking the up to 210 digits, each of the ten symmetric mappings of this group being assigned a different decimal digit. To this end, it may also be provided for the digit 0 to be assigned to the identity mapping, digits 1 through 4 to be assigned the four rotations about the midpoint of the pentagon, digits 5 through 9 to be assigned to the five reflections about the five axes of symmetry of the pentagon. If one executes two symmetric mappings one after another, then a symmetric mapping again results. Based on these allocations, one can set up the following multiplication table:

*	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	2	3	4	0	6	7	8	9	5
2	2	3	4	0	1	7	8	9	5	6
3	3	4	0	1	2	8	9	5	6	7
4	4	0	1	2	3	9	5	6	7	8
5	5	9	8	7	6	0	4	3	2	1
6	6	5	9	8	7	1	0	4	3	2
7	7	6	5	9	8	2	1	0	4	3
8	8	7	6	5	9	3	2	1	0	4
9	9	8	7	6	5	4	3	2	1	0

With the assistance of this table, the 210 digits are linked to one single digit in that, utilizing the result from the previous operation as a row indicator and utilizing the next digit as a column indicator, the next result in the table is read off successively until all digits are considered. The last result forms the desired digit of the PIN.

Exemplary embodiments of the present invention are represented by several figures in the drawing and are elucidated in the following description. The figures show:

Figure 1 a diagram for generating a customer-specific binary code;

Figure 2 a diagram for generating a PIN through conversion to a decimal number;

Figure 3 a diagram for generating a PIN by a digit-by-digit conversion into decimal numbers;

Figure 4 a diagram for generating a PIN by a digit-by-digit conversion, including modulus formation; and

Figure 5 a diagram for generating a PIN by reducing hexadecimal numbers with the assistance of mathematical groups.

Identical or corresponding parts are provided with the same reference numerals in the figures.

Figure 1 depicts a flow diagram for converting personal data D_c of a customer using a secret key K into a binary number B of L bits length. The binary number B is part of the 64-bit long encryption result, which was generated from the customer data D_c using the DES algorithm.

If the length of the binary number B equals 13, and if the number of the PIN digits to be generated equals 4, then the PIN, as shown in Figure 2, can be generated by interpreting the binary number B as decimal number D by adding a constant C thereto. The constant is to be selected such that the PIN does not have any leading zeros. In this manner, 8192 different PINS can be generated, which are absolutely uniformly distributed over the number domain in question.

Figure 3 depicts how a binary number of length 13 can be converted into a PIN in that for each digit of the PIN to be generated, a number of bits of the binary number is converted into a decimal number, and a constant C is added to the resultant number D , to avoid having leading zeros of the PIN.

In this manner, 7777 different PINS may be generated, which are absolutely uniformly distributed over the number domain in question.

5 Another possibility for generating nearly equally distributed
PINS from a binary number B is illustrated in Figure 4. The
binary number B has 52 digit positions. To generate the four-
digit PIN, the binary number B is subdivided into four
subsets, which, in the example, have the same length. Each of
10 these subsets is interpreted as a decimal number. The first
digit of the PIN is derived as a remainder of a division of
the first decimal number by 9. The following digits of the PIN
are derived in each case as a remainder of a division of the
following decimal number by 10. In this manner, 9000 different
15 PINS may be generated, which are absolutely uniformly
distributed.

From the personal data Dc of a customer, as shown in Figure 5,
a sequence of 210 hexadecimal digits is generated with the
assistance of a secret key and a random-number generator, in
that, for example, an encryption result of the DES algorithm
20 from Figure 1 is again encrypted using the algorithm, and so
forth. The 14 64-digit binary codes resulting therefrom are
converted into 14 hexadecimal numbers Hi, each having 16
digits. Lined up, this yields 224 hexadecimal digits, of which
25 210 enter into the generation of the PIN.

There are 210 different possibilities fi for mapping the set
of 16 hexadecimal digits into the set of the 10 decimal
digits. Therefore, each of the 210 hexadecimal digits is
converted using a different one of these mappings into a
30 decimal digit di. In order to produce a digit Zi of a PIN from
the 210 decimal digits, they are successively linked using the
group operation F of any arbitrary ten-element mathematical
group; the last result is the sought after digit. Thus, the
previously non-uniform, statistical distribution of the 210

decimal digits is evened out. The entire process is repeated for each of the digit positions Z2 through Z4 of the PIN.

5 Analogously for the first digit of the PIN, 36 hexadecimal digits are generated, which are mapped with every other one of the 36 possible mappings of the hexadecimal digits into the set of the digits 1 through 9, into a digit between 1 and 9. The 36 decimal digits are linked to the first digit of the PIN using the group operation of any arbitrary mathematical group of the order 9. This enables 9000 different PINs to be
10 generated which are nearly uniformly distributed. In generating 10^5 PINs, the maximum non-uniformities amounted to about 1.5 percent. This does not significantly raise the probability of a PIN being accidentally correctly guessed as compared to the theoretical minimum value. Thus, the method
15 functions very reliably.

All mathematical groups having ten elements are fundamentally suited for use with this method. Known representatives include the additive group of the integers modulo 10, $Z_{10,+}$, the multiplicative group of the integers modulo 11, Z_{11}^* , as well
20 as the group of the symmetric mappings of a regular pentagon D5, the so-called dihedral group. In the last instance, one decimal digit, which may be used for the calculation, is assigned to each of the individual elements of the group.

What is claimed is:

1. A method for generating a personal identification number (PIN), made up of a number of N decimal digits, to be used for money cards and other devices requiring security, from a binary number having L digits, in particular from a binary code specific to an individual, wherein the PINs are generated such that they are randomly uniformly distributed over the available number domain.
2. The method as recited in Claim 1, wherein the first n_1 digits of the binary number (B) are converted in generally known fashion into a decimal number d_1 , the predefinable natural number n_1 being selected so as to yield a natural number z_1 such that the quotient $2^{n_1}/(z_1 \cdot 9)$ is close to 1; and the first decimal digit of the PIN receives the value d_1 modulo 9; $N-1$ further groups of further n_2 digits of the binary number (B) are converted each time in generally known fashion into $N-1$ decimal numbers d_2 through d_N , the predefinable number n_2 being selected so as to yield a natural number z_2 such that the quotient $2^{n_2}/(z_2 \cdot 10)$ is close to 1, to satisfy the condition: $0 \leq 2^{n_2} \text{ modulo } 10 < 3$, and the decimal digits 2 through N of the PIN receive the values d_i modulo 10, $i=2$ through N .
3. The method as recited in Claim 2, wherein n_1 and $n_2 \leq 16$ are predefined.
4. The method as recited in one of the preceding claims, wherein $N=4$ is selected.
5. The method as recited in one of the preceding claims, wherein the binary number (B) has the length $L=16$, $N=4$ is predefined, and $n_1=n_2=4$ are predefined.

6. The method as recited in Claim 1,
wherein the binary number (B) has the length $L=3*n3$, $n3$ groups of three digits of the binary number (B) are converted in generally known fashion into $n3$ decimal digits to generate the $n3$ digits of the PIN, $n3$ being a natural number.
7. The method as recited in Claim 1,
wherein the binary number (B) is fully converted, in generally known fashion, into a decimal number in order to generate the PIN, and, if necessary, a correction value of such kind is added to the resultant decimal number that the first digit of the decimal number becomes unequal to zero, the digits of the result forming the digits of the PIN.
8. The method as recited in Claim 7,
wherein the binary number (B) has a length L of 13, the generated decimal number has four digits, and a preset value greater than 999 and smaller than 1807 is added to the decimal number.
9. The method as recited in Claim 8,
wherein the set of numbers 0 through 8191 is allocated to $n5$ subsets $M1, \dots, Mn5$, and a preset value d_i is added to the generated decimal number if it is an element of the set M_i , it holding that $999 < d1 < d2 < \dots < dn5 < 1809$, and $n5$ being a natural number.

10. The method as recited in Claim 7,
wherein the binary number (B) has a length L of 16, the
generated decimal number has five digits, and a preset
value greater than 9999 and smaller than 34465 is added
to the decimal number.
11. The method as recited in Claim 10,
wherein the set of numbers 0 through 65535 is allocated
to n_5 subsets M_1, \dots, M_{n_5} , and a preset value d_i is added
to the generated decimal number if it is an element of
the set M_i , it holding that $9999 < d_1 < d_2 < \dots < d_{n_5} < 34465$, and
 n_5 being a natural number.

12. The method as recited in Claim 1,
wherein to generate the first digits of the PIN, the
following steps are executed:
- a pseudo-random number composed of up to 36 hexadecimal
digits is generated from the binary number (B) of length
L;
 - each hexadecimal digit of this number is converted using
one different one out of the 36 possible different
mathematical mappings of hexadecimal digits into the
digits 1 through 9, into a digit of the digits 1 through
9;
 - to even out the probability of the particular PIN digit
occurring, the up to 36 decimal digits of the thus
generated number are linked in a mathematical operation
to form a decimal digit unequal to zero, which represents
the first digit of the PIN;

and the following steps are executed for the second and each
following digit of the PIN to be generated:

- a pseudo-random number composed of up to 210 hexadecimal
digits is generated from the binary number (B) of length
L;
- each hexadecimal digit of this number is converted into
one decimal digit using each time one different one out

of the 210 possible mathematical mappings of hexadecimal digits into decimal digits;

- to average out the probability of the particular PIN digit occurring, the up to 210 decimal digits of the thus generated number are linked in a mathematical operation to form a decimal digit, which represents the particular digit of the PIN.
13. The method as recited in Claim 12, wherein the first digit of the PIN is generated in that the up to 36 digits are linked using the group operation of any arbitrary mathematical group of the order 9, and the second and the following digits of the PIN are generated, in that the up to 210 digits are linked using the group operation of any arbitrary mathematical group of the order 10.
 14. The method as recited in Claim 13, wherein the additive group of the integers modulo 10 are used to link the up to 210 digits.
 15. The method as recited in Claim 13, wherein the multiplicative group of the integers modulo 11 are used to link the up to 210 digits.
 16. The method as recited in Claim 13, wherein the group of the symmetric mappings of a regular pentagon (dihedral group) is used to link the up to 210 digits, each of the ten symmetric mappings of this group being assigned a different decimal digit.
 17. The method as recited in Claim 16, wherein the digit 0 is assigned to the identity mapping, the digits 1 through 4 to the four rotations about the midpoint of the pentagon, and the digits 5 through 9 to the five reflections about the five axes of symmetry of the pentagon.

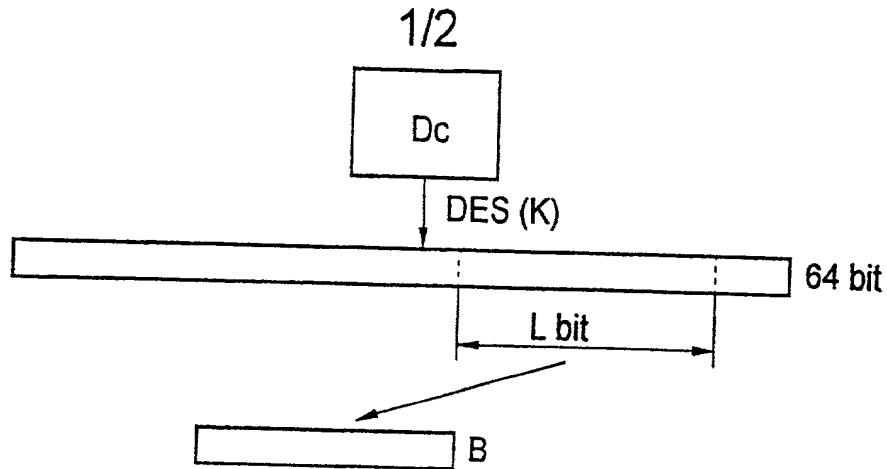


Fig.1

$L = 13,$
 $N = 4,$
 $\text{PINmax-PINmin}=8192$

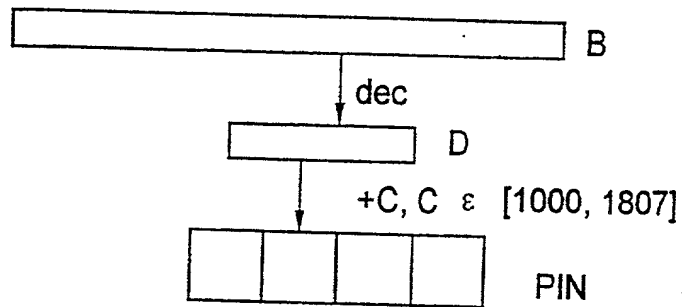


Fig.2

$L = 12,$
 $N = 4,$
 $\text{PINmax-PINmin}=7777$

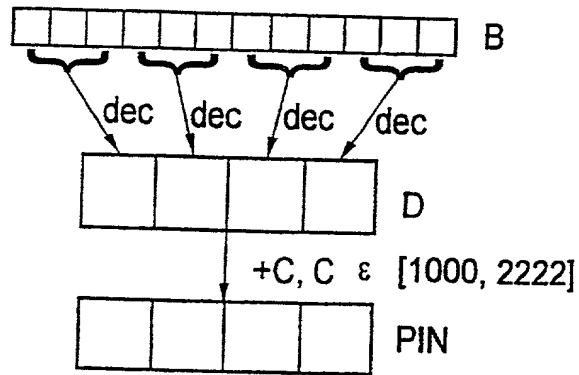


Fig.3

$L = 52,$
 $N = 4,$
 $\text{PINmax-PINmin}=9000$

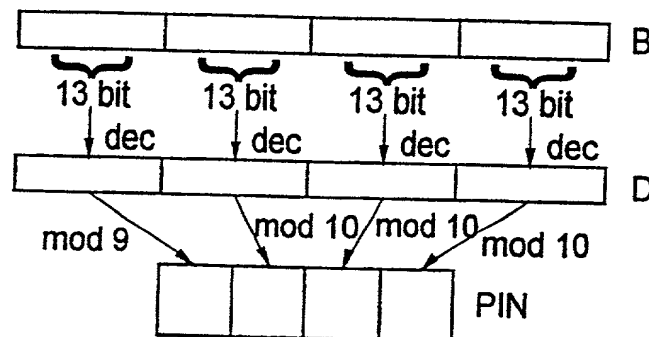


Fig.4

2/2

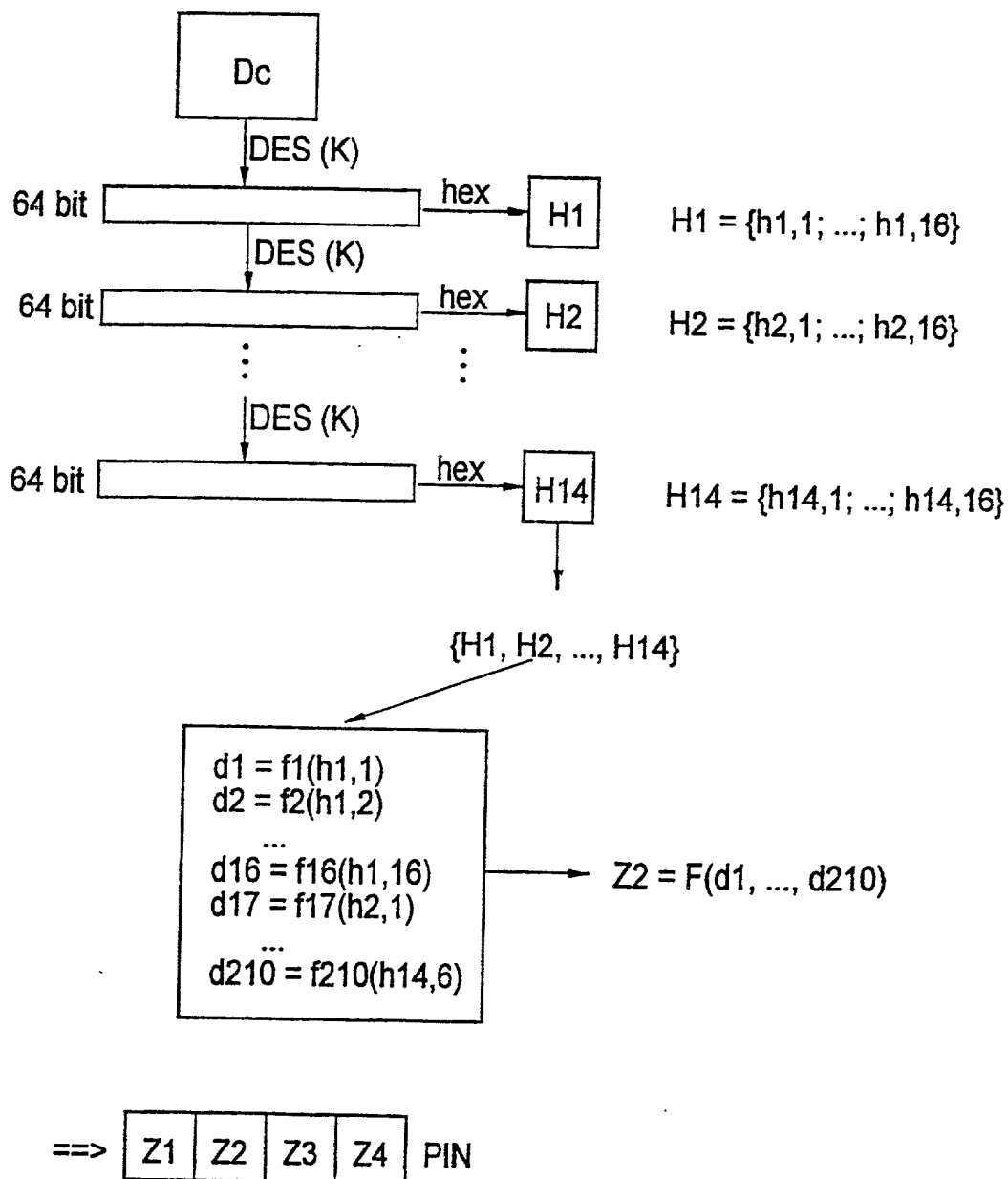
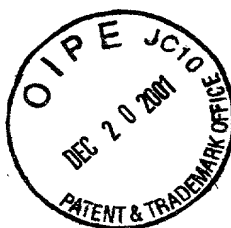


Fig.5



2345/165

DECLARATION AND POWER OF ATTORNEY

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled **METHOD FOR GENERATING IDENTIFICATION NUMBERS**, the specification of which was filed as International Application No. PCT/EP00/02481 on March 21, 2000 and filed as an application for Letters Patent in the U.S.P.T.O. on October 1, 2001.

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims.

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, § 1.56(a).

I hereby claim foreign priority benefits under Title 35, United States Code, § 119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application(s) for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

PRIOR FOREIGN APPLICATION(S)

Number	Country Filed	Day/Month/Year	Priority Claimed Under 35 USC 119
199 14 407.9	Fed. Rep. of Germany	March 30, 1999	Yes

And I hereby appoint Richard L. Mayer (Reg. No. 22,490), Gerard A. Messina (Reg. No. 35,952) and Linda M. Shudy (Reg. No. 47,084) my attorneys with full power of substitution and revocation, to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith.

Please address all communications regarding this application to:

KENYON & KENYON
One Broadway
New York, New York 10004

CUSTOMER NO. 26646

Please direct all telephone calls to Richard L. Mayer at (212) 425-7200.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful and false statements may jeopardize the validity of the application or any patent issued thereon.

Inventor: Joerg SCHWENK

100
Inventor's Signature: _____

Date: 23.11.01

Residence: ~~Suedwestring 27~~ Weissstr. 10
~~D-64807 Dieburg~~ 91239 Hemdenfeld DEU
Federal Republic of Germany

Citizenship: German

Office Address: Same as above.

Inventor: **Tobias MARTIN**

200
Inventor's Signature: Tobias Martin

Date: 21/11/2001

Residence: Spitzengaerten 1
D-35466 Rabenau-Ruddinghausen DE
Federal Republic of Germany

Citizenship: German

Office Address: Same as above.

DECLARATION AND POWER OF ATTORNEY

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled **METHOD FOR GENERATING IDENTIFICATION NUMBERS**, the specification of which was filed as International Application No. PCT/EP00/02481 on March 21, 2000.

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims.

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, § 1.56(a).

I hereby claim foreign priority benefits under Title 35, United States Code, § 119 of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application(s) for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

PRIOR FOREIGN APPLICATION(S)

Number	Country Filed	Day/Month/Year	Priority Claimed Under 35 USC 119
199 14 407.9	Fed. Rep. of Germany	March 30, 1999	Yes

Express Mail No. EL244508211US

And I hereby appoint Richard L. Mayer (Reg. No. 22,490), Gerard A. Messina (Reg. No. 35,952) and Linda M. Shudy (Reg. No. 47,084) my attorneys with full power of substitution and revocation, to prosecute this application and to transact all business in the Patent and Trademark Office connected therewith.

Please address all communications regarding this application to:

KENYON & KENYON
One Broadway
New York, New York 10004

CUSTOMER NO. 26646

Please direct all telephone calls to Richard L. Mayer at (212) 425-7200.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful and false statements may jeopardize the validity of the application or any patent issued thereon.

Inventor: **Joerg SCHWENK**

Inventor's Signature: _____

Date: _____

Residence: Suedwestring 27
D-64807 Dieburg
Federal Republic of Germany

Citizenship: German

Office Address: Same as above.

Inventor: **Tobias MARTIN**

Inventor's Signature: _____

Date: _____

Residence: Spitzengaerten 1
D-35466 Rabenau-Ruddinghausen
Federal Republic of Germany

Citizenship: German

Office Address: Same as above.